

# Fordham Intellectual Property, Media and Entertainment Law Journal

---

Volume 15 *Volume XV*  
Number 3 *Volume XV Book 3*

Article 3

---

2005

## Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions

YiJun Tian

*University of New South Wales, Australia*

Follow this and additional works at: <https://ir.lawnet.fordham.edu/iplj>



Part of the [Entertainment, Arts, and Sports Law Commons](#), and the [Intellectual Property Law Commons](#)

---

### Recommended Citation

YiJun Tian, *Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions*, 15 Fordham Intell. Prop. Media & Ent. L.J. 749 (2005).  
Available at: <https://ir.lawnet.fordham.edu/iplj/vol15/iss3/3>

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Intellectual Property, Media and Entertainment Law Journal by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact [tmelnick@law.fordham.edu](mailto:tmelnick@law.fordham.edu).

---

# Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions

Cover Page Footnote

Jill McKeough

# Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions

YiJun Tian\*

INTRODUCTION .....	750
I. U.S. AND INTERNATIONAL ANTI-CIRCUMVENTION LAWS ....	753
A. <i>Requirements in the WIPO Internet Treaties</i> .....	753
B. <i>Application of Anti-Circumvention Laws in the U.S.</i> ....	755
1. Background .....	755
2. Rule I: Provisions for Banning the Acts of Circumventing Access-Controls.....	757
3. Anti-Devices Provisions.....	758
a) Rule II: Section 1201(a)(2)—Forbidding Devices that Circumvent Access Controls .....	759
b) Rule III: Section 1201(b)—Forbidding Devices Which Circumvent Right Controls ...	759
4. Exceptions for Anti-Circumvention Rules .....	762
a) Exceptions for § 1201(a)(1)(A).....	763
b) Exceptions for Anti-Devices Provisions: §§ 1201(a)(2) and 1201(b) .....	765
c) Other General Provisions that Limit Anti- Circumvention Rules.....	765
II. THE PROBLEMS WITH THE ANTI-CIRCUMVENTION RULES IN THE DMCA .....	766
A. <i>General Problems &amp; Why There Is a Need for</i>	

---

\* PhD Candidate, Faculty of Law, University of New South Wales, Australia; Visiting Scholar, Faculty of Law, University of Washington, USA. I would like to thank my supervisor Professor Jill McKeough, for her comments and help with earlier drafts of this paper.

750	<i>FORDHAM INTELL. PROP. MEDIA &amp; ENT. L.J.</i>	[Vol. 15:749]
	<i>Anti-Device Rules</i> .....	767
B.	<i>Problem I: Fair Use vs. Different Treatments in Anti-Circumvention Rules</i> .....	769
C.	<i>Problem II: Overly Narrow Exceptions &amp; Lack of a General Purpose Exception for Other Legitimate Reasons</i> .....	772
D.	<i>Problem III: "Para-Copyright" Provisions &amp; Misuse of Anti-Circumvention Rights</i> .....	774
III.	<b>FUTURE ANTI-CIRCUMVENTION RULES: HETEROGENEOUS SOLUTIONS</b> .....	779
A.	<i>Broader Exceptions: Fair Circumvention Doctrine (A Statutory/Common Law Solution)</i> .....	779
B.	<i>Controlling Technological Measures to Protect Users: Proposed Legal Solutions &amp; Market Solutions</i> .....	782
C.	<i>Predictable Problems on Enforcement of New Doctrine &amp; Possible Legal Solutions</i> .....	785
D.	<i>General Advice for Future Legislators &amp; the Multi-Level Role of Copyright Law in Future Legal Reform</i> .....	786
	<b>CONCLUSION</b> .....	788

## INTRODUCTION

With the dramatic development of Information Communication Technology (ICT), the Internet has become a major source for the dissemination of intellectual property. The Internet not only "changed the [traditional] rules of distribution and dissemination of information,"<sup>1</sup> it brought great challenges to traditional business models and legal enforcement of copyrights. The development of digital technology has greatly reduced the cost of making multiple copies and has facilitated the dissemination of online materials. This brings great conveniences, but also enables widespread piracy.<sup>2</sup>

<sup>1</sup> Shantanu Rastogi, *WCT & WPPT Background and Purpose* (2003), at [http://www.techlex.org/library/wct\\_wppt.pdf](http://www.techlex.org/library/wct_wppt.pdf).

<sup>2</sup> See, e.g., Jennifer Newton, Note, *Global Solutions to Prevent Copyright Infringement of Music Over the Internet: The Need to Supplement the WIPO Internet*

Many copyright owners fear that the application of these new technologies may cause "a loss of control" over their copyrighted works.<sup>3</sup> They believe that traditional copyright law is not strong enough to protect their rights on the Internet, so they have tried to apply technical measures to defend themselves.<sup>4</sup> However, technological measures are not always effective.<sup>5</sup> As one commentator pointed out, "as soon as the copyright industry seals its products under a protective wrap, hackers will restore free access."<sup>6</sup> Indeed, technical protection measures do increase a copyright holder's protection, but technology alone seems insufficient to achieve complete control of protected content.<sup>7</sup> Gradually, copyright industries have realized this and have started to seek legal support from both international and domestic legislation.

The concerns of copyright industries were considered at an international conference of the World Intellectual Property Organization (WIPO) in Geneva in December 1996.<sup>8</sup> In order "to update world copyright law in response to challenges presented by digital technology,"<sup>9</sup> the conference "adopted two related treaties, the WIPO Copyright Treaty [(WCT)], and the WIPO Performances and Phonograms Treaty [(WPPT)]," also referred to as the "WIPO Internet Treaties."<sup>10</sup> The treaties included a new *sui generis*

---

*Treaties with Self-Imposed Mandates*, 12 IND. INT'L & COMP. L. REV. 125, 125 (2001) ("[T]he expansion of the Internet provides a huge market for piracy.").

<sup>3</sup> Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1097 (2003).

<sup>4</sup> See Haimo Schack, *Anti-Circumvention Measures and Restrictions in Licensing Contracts as Instruments for Preventing Competition and Fair Use*, 2002 U. ILL. J.L. TECH. & POL'Y 321, 322 (2002).

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> Newton, *supra* note 2, at 149–50.

<sup>8</sup> See *WIPO Copyright Treaty* ("WCT"), art. 11, CRNR/DC/94 (Dec. 23, 1996), <http://www.wipo.int/documents/en/diplconf/distrib/pdf/94dc.pdf>; *WIPO Performances and Phonograms Treaty* ("WPPT"), art. 18, CRNR/DC/95 (Dec. 23, 1996), <http://www.wipo.int/documents/en/diplconf/distrib/pdf/95dc.pdf>.

<sup>9</sup> Brian Bolinger, Comment, *Focusing on Infringement: Why Limitations on Decryption Technology Are Not the Solution to Policing Copyright*, 52 CASE W. RES. L. REV. 1091, 1092 (2002).

<sup>10</sup> See Jane C. Ginsburg, *Achieving Balance in International Copyright Law*, 26 COLUM.-VLA J.L. & ARTS 201, 201 (2003) (reviewing JÖRG REINBOTHE AND SILKE VON LEWINSKI, *THE WIPO TREATIES 1996: THE WIPO COPYRIGHT TREATY AND THE WIPO*

provision on protecting anti-circumvention measures, and required all member states to provide “adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with their rights in copyright works.”<sup>11</sup> However, “the Treat[ies] [did] not provide enforcement mechanisms,” and leave “enforcement . . . up to the individual countries.”<sup>12</sup>

Over the past few years (after the WIPO conference), copyright industries have already successfully lobbied both U.S. and foreign legislatures to adopt anti-circumvention rules to protect technological measures from being hacked.<sup>13</sup> Moreover, establishing anti-circumvention provisions also became one of the requirements in some regional treaties, such as the bilateral Free Trade Agreement.<sup>14</sup> This Article will first examine the basic requirements for anti-circumvention legislation in the WIPO Internet Treaties.<sup>15</sup> Then, it will focus on the detailed anti-circumvention rules and corresponding exceptions in the U.S.’s *Digital Millennium Copyright Act* (DMCA).<sup>16</sup> It will identify the major problems of the DMCA anti-circumvention provisions (such as failing to protect fair use, and overly narrow exceptions)<sup>17</sup> through an analysis of DMCA related case law.<sup>18</sup> Finally, this Article will suggest reforms for the U.S. anti-circumvention legislation by drawing on experience from existing domestic legislation in the U.S. and abroad (particularly Germany and

---

PERFORMANCES AND PHONOGRAMS TREATY: COMMENTARY AND LEGAL ANALYSIS (2002)).

<sup>11</sup> See Jacqueline Lipton, *Copyright in the Digital Age: A Comparative Survey*, 27 RUTGERS COMPUTER & TECH. L.J. 333, 338 (2001); see also *WCT*, *supra* note 8, art. 11; *WPPT*, *supra* note 8, art. 18.

<sup>12</sup> Newton, *supra* note 2, at 144.

<sup>13</sup> Pamela Samuelson, *DRM {and, or, vs.} the Law*, COMM. OF THE ACM, Apr. 2003, at 41, [http://www.sims.berkeley.edu/~pam/papers/acm\\_v46\\_p41.pdf](http://www.sims.berkeley.edu/~pam/papers/acm_v46_p41.pdf) (hereinafter Samuelson, *DRM*).

<sup>14</sup> See, e.g., Australia-United States Free Trade Agreement, ch. 17 (Intellectual Property Rights), [http://www.dfat.gov.au/trade/negotiations/us\\_fta/final-text/index.html](http://www.dfat.gov.au/trade/negotiations/us_fta/final-text/index.html) (May 18, 2004).

<sup>15</sup> See *infra* notes 28–36 and accompanying text.

<sup>16</sup> 17 U.S.C. §§ 1201–1205 (2002).

<sup>17</sup> See *infra* notes 104–90 and accompanying text.

<sup>18</sup> See *id.*

Japan).<sup>19</sup> It concludes that a “fair circumvention” doctrine/exception should be established and a more heterogeneous method (where statutes, the discretionary power of the courts, soft laws, market forces, and government agencies all work together)<sup>20</sup> should be applied to deal with the challenges brought by anti-circumvention law in the digital era.<sup>21</sup> It will also identify a trend towards the separation of the anti-circumvention rules from copyright, and recommend that copyright law plays an important role during the transition period.<sup>22</sup>

## I. U.S. AND INTERNATIONAL ANTI-CIRCUMVENTION LAWS

### A. *Requirements in the WIPO Internet Treaties*

The WIPO Internet Treaties, adopted in December 1996, are “the first international treaties that deal specifically with copyright infringement over the Internet.”<sup>23</sup> Regarding the issue of technological protection measures, each of the WIPO Internet Treaties contains virtually identical language, obligating member countries to prohibit circumvention of technological measures that are employed to protect copyrighted works.<sup>24</sup>

Specifically, article 11 of the WCT sets out the following obligations concerning technological measures:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in

---

<sup>19</sup> See *infra* notes 189–211 and accompanying text.

<sup>20</sup> See *infra* notes 178–211 and accompanying text.

<sup>21</sup> See *infra* Part III.D.

<sup>22</sup> See *infra* Parts II.D, III.B.

<sup>23</sup> Newton, *supra* note 2, at 143.

<sup>24</sup> *Id.*; see U.S. COPYRIGHT OFFICE, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 3 (1998), at <http://www.loc.gov/copyright/legislation/dmca.pdf> (hereinafter COPYRIGHT OFFICE DMCA SUMMARY). The U.S. Copyright Office observed that these obligations serve as technological adjuncts to the exclusive rights “granted by copyright law.” *Id.*

respect of their works, which are not authorized by the authors concerned or permitted by law.<sup>25</sup>

Article 18 of the WPPT contains nearly identical language, and sets out obligations for protecting technological measures that are used by performers or producers of phonograms.<sup>26</sup>

Through these provisions, the WIPO Internet Treaties advise member countries to introduce into their domestic legislation anti-circumvention provisions designed to protect copyrighted works in digital domain.<sup>27</sup> These provisions show that the drafters of the Internet Treaties were very careful not to eliminate any existing provision that the Berne Convention had established,<sup>28</sup> as exemplified by the clause in article 11 of the WCT providing that the treaty obligations do “not go further than the scope of copyright.”<sup>29</sup> Therefore, the permitted privileges of users (such as fair use) under traditional copyright law may still prevail over the anti-circumvention provisions.<sup>30</sup>

Although the WIPO Internet Treaties provide legal remedies for the circumvention of technological measures employed on protected works, they remain silent on enforcement mechanisms and leave enforcement to individual countries.<sup>31</sup> Nor do they pinpoint any specific technological measures that must be incorporated in the domestic laws of member countries.<sup>32</sup> Rather, the treaties give the member states freedom to apply their own domestic laws to deal with the anti-circumvention issues.

---

<sup>25</sup> See *WCT*, *supra* note 8, art. 11.

<sup>26</sup> See *WPPT*, *supra* note 8, art. 18 (“Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.”).

<sup>27</sup> Rastogi, *supra* note 1, at 5.

<sup>28</sup> Newton, *supra* note 2, at 144.

<sup>29</sup> Schack, *supra* note 4, at 323. Schack also notes that “[p]rotection of technological measures is mandated only insofar as they are intended to protect the copyright owners’ exploitation rights, but not as to acts ‘permitted by law.’” *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> See *supra* note 8 and accompanying text.

<sup>32</sup> Rastogi, *supra* note 1, at 5.



*B. Application of Anti-Circumvention Laws in the U.S.*

This Article primarily will focus on the DMCA as representative of anti-circumvention rules in most countries. The reason is that “although dozens of other countries have agreed to incorporate anti-circumvention into their laws, the ‘United States has taken the lead in terms of enacting “anti-circumvention” provisions into its domestic law.”<sup>33</sup>

*1. Background*

As introduced above, the WIPO Internet Treaties established the minimum standards for member countries to establish anti-circumvention laws to protect copyrighted materials.<sup>34</sup> Over the past few years, most member states adapted their copyright law, and some, including the United States, granted more protection than the treaties required.<sup>35</sup>

In response to the WIPO Internet Treaties and industry concerns, the U.S. Congress passed the DMCA in 1998.<sup>36</sup> The DMCA not only prohibits acts of circumvention,<sup>37</sup> it also grants absolute protection to technological measures that control access to a work or protect the exclusive rights of a copyright holder.<sup>38</sup>

The DMCA provides three principal rules for preventing the circumvention of technological measures protecting copyrighted works. Section 1201(a)(1) prohibits circumventing a technological measure that controls access to a protected work (access

---

<sup>33</sup> Terri Branstetter Cohen, Note, *Anti-Circumvention: Has Technology's Child Turned Against its Mother?*, 36 VAND. J. TRANSNAT'L L. 961, 984 (2003) (citing Jacqueline Lipton, *E-Commerce in the Digital Millennium: The Legal Ramifications of the DMCA and Business Method Patents*, 27 RUTGERS COMPUTER & TECH. L.J. 333, 359 (2001)). Cohen observes that “[e]valuating these portions of the DMCA best demonstrates the practical effects of implementing anti-circumvention provisions.” *Id.*

<sup>34</sup> See, e.g., *supra* note 11 and accompanying text.

<sup>35</sup> See, e.g., Cohen, *supra* note 33, at 986 (“Clearly, the DMCA enacts a broad interpretation of the WIPO Copyright Treaty’s anti-circumvention provisions because it applies to acts beyond actual technical circumvention and to those who have a legal right to use the works.”); cf. Schack, *supra* note 4, at 323 (stating that the U.S. “WIPO delegates in Geneva had argued for a stricter protection.”).

<sup>36</sup> See, e.g., Cohen, *supra* note 33, at 982–83.

<sup>37</sup> 17 U.S.C. § 1201(a)(1) (2002).

<sup>38</sup> *Id.* §§ 1201(a)(2), (b)(1); see also Schack, *supra* note 4, at 323.

controls).<sup>39</sup> Section 1201(a)(2) forbids the trafficking or distribution of devices that facilitate circumvention of technological measures used to control access to a protected work (access controls).<sup>40</sup> Section 1201(b) prohibits trafficking in devices that circumvent technological control measures used to protect the exclusive rights of copyright holders (right controls/post-access controls).<sup>41</sup> These rules will be explored in greater detail in the following sections.<sup>42</sup>

Because § 1201(a)(2) and § 1201(b) both regulate “technologies, product[s], service[s], device[s], component[s], [and] part[s] thereof” having circumvention-enabling capabilities, they are often referred to as “Anti-Device” provisions.<sup>43</sup> As to the scope of the “device,” § 1201 explicitly states “no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof”<sup>44</sup> if it falls within any one of the following three categories:

- It is primarily designed or produced to circumvent;
- It has only a limited commercially significant purpose or use other than to circumvent; or
- It is marketed for use in circumventing.<sup>45</sup>

Remedies are specified in sections 1203 and 1204 of the DMCA. Section 1203 provides civil remedies, allowing any person who is injured by violation of said provisions (either § 1201(a)(1)(A), § 1201(a)(2), or § 1201(b)) to bring a civil action in federal court and sue for damages, injunctive relief, and attorney fees.<sup>46</sup> Section 1204 provides the penalties for criminal offenses.<sup>47</sup>

---

<sup>39</sup> 17 U.S.C. § 1201(a)(1); Lipton, *supra* note 11, at 342.

<sup>40</sup> 17 U.S.C. § 1201(a)(2); Pete Singer, Comment, *Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act*, 28 U. DAYTON L. REV. 111, 116 (2002).

<sup>41</sup> 17 U.S.C. § 1201(b).

<sup>42</sup> See *infra* Parts I.B.2–3.

<sup>43</sup> Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 534 (1999) (hereinafter Samuelson, *Anti-Circumvention*); see also Lipton, *supra* note 11, at 343.

<sup>44</sup> 17 U.S.C. § 1201(a)(2), (b)(1).

<sup>45</sup> See COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 4.

<sup>46</sup> Samuelson, *DRM*, *supra* note 13, at 42.

This Article will next examine the three anti-circumvention rules in more detail, and provide examples of activities that would violate each rule.

## 2. Rule I: Provisions for Banning the Acts of Circumventing Access-Controls

Section 1201(a)(1)(A) of the DMCA prohibits circumventing “a technological measure that effectively controls access to a work protected under this title.”<sup>48</sup> As to the meaning of “circumventing a protected work,” § 1201 includes actions as varied as descrambling a scrambled work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing a technological measure without the permission of the copyright owner.<sup>49</sup> Further, § 1201 defines a technological measure that “effectively controls access to a work” as a measure that “requires the application of certain information, or a process or treatment, with the authority of the copyright owner, to gain access to the work.”<sup>50</sup>

---

<sup>47</sup> 17 U.S.C. § 1204 (2002). Criminal offenses and penalties include:

(a) IN GENERAL.—Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain—

(1) shall be fined not more than \$500,000 or imprisoned for not more than 5 years, or both, for the first offense; and

(2) shall be fined not more than \$1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.

(b) LIMITATION FOR NONPROFIT LIBRARY, ARCHIVES, EDUCATIONAL INSTITUTION, OR PUBLIC BROADCASTING ENTITY.—Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(g)).

(c) STATUTE OF LIMITATIONS.—No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.

*Id.*; see also COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 7; Herbert J. Hammond et al., *The Anti-Circumvention Provision of the Digital Millennium Copyright Act*, 8 TEX. WESLEYAN L. REV. 593, 599–601 (2002).

<sup>48</sup> Hammond et al., *supra* note 47 at 596. “[B]y ‘this title,’ the provision is referring to the 1976 Copyright Act codified in Title 17 of the U.S. Code.” *Id.* at 596.

<sup>49</sup> 17 U.S.C. § 1201(a)(3)(A); see also Christine Jeanneret, *The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance*, 12 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 157, 164 (2001).

<sup>50</sup> 17 U.S.C. § 1201(a)(3)(B).

For instance, an effective technological measure for access control could be the password page on a database website, such as the home page of the Westlaw legal database. In order to obtain the password to access the articles in the database, any institution or individual user will be required to pay a license fee. If a user who has not paid the license fee deactivates or avoids the Westlaw password page and accesses the articles in the database, then the user will violate § 1201(a)(1)(A).

Out of concern that § 1201(a)(1)(A) might have a negative impact on non-infringing uses of copyrighted works, the U.S. Congress decided that this rule should not take effect until October 2000 (two years after the DMCA was enacted).<sup>51</sup> The Library of Congress was instructed to conduct a regular study into the impact of this rule on non-infringing uses of copyrighted works. Congress also created seven very specific exceptions to the rule, along with several other more general limitations.<sup>52</sup> This Article will later discuss the exceptions and limitations in further detail.

### 3. Anti-Devices Provisions

“Section 1201 divides technological measures into two categories: measures that prevent unauthorized *access* to a copyrighted work [access controls] and measures that prevent unauthorized *copying*<sup>53</sup> of a copyrighted work [right controls/post-access controls].”<sup>54</sup> Such a division helps to understand the difference between the two anti-devices rules in § 1201(a)(2) and § 1201(b).

---

<sup>51</sup> Pamela Samuelson, *Towards More Sensible Anti-Circumvention Regulations* 3 (2000), at <http://www.sims.berkeley.edu/~pam/papers/fincrypt2.pdf> [hereinafter Samuelson, *More Sensible Regulations*].

<sup>52</sup> *Id.*

<sup>53</sup> See COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 4 n.2 (“‘Copying’ is used in this context as a short-hand for the exercise of any of the exclusive rights of an author under section 106 of the Copyright Act. Consequently, a technological measure that prevents unauthorized distribution or public performance of a work would fall in this second category.”).

<sup>54</sup> *Id.* at 3–4.

a) Rule II: Section 1201(a)(2)—Forbidding Devices that Circumvent Access Controls

Section 1201(a)(2) provides that “[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic” in any devices or technology that is primarily designed or produced to circumvent “access-controls.”<sup>55</sup> Sections 1201(a)(2) and 1201(a)(1)(A) both deal with “access-control” measures,<sup>56</sup> but they differ in that the former forbids trafficking in devices that circumvent access controls, while the latter bans the act of circumventing access controls.<sup>57</sup> Again using Westlaw as an example, if a person publicly offers a special software which has the sole function of enabling a user to access the Westlaw database without any password or authorization from Westlaw, then the offeror would violate § 1201(a)(2).<sup>58</sup> However, the person who uses the special software to circumvent the Westlaw password page, without any authorization from Westlaw, violates § 1201(a)(1)(A).<sup>59</sup>

b) Rule III: Section 1201(b)—Forbidding Devices Which Circumvent Right Controls

Whereas § 1201(a)(2) prohibits trafficking in devices that circumvent access control, § 1201(b) provides that “no person shall manufacture, import, offer to the public, provide, or otherwise traffic” in any devices or technologies designed or produced to circumvent technological measures that protect the exclusive rights of copyright holders in the Copyright Act.<sup>60</sup> In other words, it prohibits circumvention of “right-controls measures” that copyright holders employ to prevent unauthorized reproduction or other forms of copyright infringement, i.e. those

<sup>55</sup> Some commentators noted that the U.S. Congress modeled this provision from its existing laws banning “black boxes,” which descramble cable-television and satellite-cable services. Hammond et al., *supra* note 47, at 597.

<sup>56</sup> See 17 U.S.C. § 1201(a)(2), (a)(1)(A) (2002).

<sup>57</sup> See *id.*; see also Singer, *supra* note 40, at 116–17. Singer provides a more general example (eBook website) to explain the difference of the two sections. Singer, *supra* note 40, at 117.

<sup>58</sup> See 17 U.S.C. § 1201(a)(2).

<sup>59</sup> See 17 U.S.C. § 1201(a)(1)(A).

<sup>60</sup> See 17 U.S.C. § 1201(b) (2002).

measures “designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright.”<sup>61</sup> Section 1201(b)(1) only applies to persons who have obtained lawful access to a copy of the work, but thereafter manufacture, or distribute the prohibited devices enabling the circumvention of right-control measures (e.g., an anti-copy measure) contained in the protected copy.<sup>62</sup> Because this section only applies to users’ actions after they have lawfully accessed the technically protected works, some commentators refer to the provision in § 1201(b) as “post-access copyright control.”<sup>63</sup>

Unlike § 1201(a)(1)(A), which bans circumventing access-controls, § 1201(b) does not ban circumventing post-access copyright controls, it only deals with the trafficking or distribution of devices that circumvent post-access copyright controls.<sup>64</sup> Thus, once a user obtains lawful access to a copyrighted work, even if the user circumvents technological measures (either access control or rights control measures), the user would not violate any provision in § 1201.<sup>65</sup>

Many websites allow the user to access online documents (no access-controls), but they do not allow users to download or print a copy of these documents. A typical example would be the “Australian Guide to Legal Citation” (AGLC) website.<sup>66</sup> The declaration on the homepage of AGLC explicitly states that the book “AGLC” may be downloaded as a PDF document “for

<sup>61</sup> Singer, *supra* note 40, at 118.

<sup>62</sup> As such, one commentator argued that the DMCA clearly enacts a broad interpretation of the WIPO Copyright Treaty’s anti-circumvention provisions, because § 1201 not only applies to “acts beyond actual technical circumvention” but also applies to “those who have a legal right to use the works.” See Cohen, *supra* note 33, at 986.

<sup>63</sup> Singer, *supra* note 40, at 118. For some examples of “post-access copyright control” technologies, including anti-copying, anti-distributing, anti-display codes technologies, see *id.*

<sup>64</sup> *Id.*; see also COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 3–4.

<sup>65</sup> David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 689 (2000). Likewise, Ginsburg argues that “section 1201(b) . . . does not prohibit direct acts of circumvention; the technologically adept user thus faces no liability under that section [§ 1201(b)].” See Jane C. Ginsburg, *Copyright Legislation for the Digital Millennium*, 23 COLUM.-VLA J.L. & ARTS 137, 143 (1999) (hereinafter Ginsburg, *Copyright Legislation*).

<sup>66</sup> Melbourne University Law Review, *Australian Guide to Legal Citation*, <http://mulr.law.unimelb.edu.au/aglc.asp> (last updated Sept. 24, 2004).

viewing only,” and if users want hard copies of the AGLC, they must order it from the Melbourne University Law Review Association.<sup>67</sup> Indeed, if a user downloads and opens the AGLC e-book, the user will find the “print” button has been disabled.

Assume a hypothetical AGLC user searches the Internet and finds special software or a device that has the sole function of circumventing rights-control measures that prevent users from printing PDF documents. Then, suppose that the user implemented the software/device to break the rights-control measures and printed out the AGLC PDF document. In this hypothetical, the person who publicly offers the circumvention software/device would be liable for the violation of § 1201(b),<sup>68</sup> while the user would not be liable. Specifically, the action that the user conducted does not constitute a violation of § 1201 for following reasons:

- First, the AGLC website allows users to view the e-book “AGLC” online freely, so the user does not need to circumvent any access-control measures to view the e-book, and he/she does not violate § 1201(a)(1)(A).<sup>69</sup>
- Second, the user just conducted an act of circumventing AGLC anti-copying technological measure (a right-control measure). He/she has not trafficked or distributed any device/technology of circumventing technical measure for both access-controls and right-controls that are banned by § 1201(a)(2) and § 1201(b)(1), so he/she does not violate “anti-device” provisions either.<sup>70</sup>

However, the user could be held liable for copyright infringement under the Copyright Act<sup>71</sup> if the user disables the copy-control measures and prints out the AGLC documents or distributes the documents to others (whether in hardcopy version

---

<sup>67</sup> See *id.*

<sup>68</sup> The software provider has conducted the action banned by § 1201(b). He or she manufactured and distributed a device or technology designed to circumvent technological measures that protect reproduction rights of copyright holders. See 17 U.S.C. § 1201(b) (2002).

<sup>69</sup> See Nimmer, *supra* note 65, at 690 n.88.

<sup>70</sup> *Id.*

<sup>71</sup> 17 U.S.C. § 501 (2002).

or printable PDF version). This would infringe the reproduction and distribution rights of the copyright holder.<sup>72</sup> Moreover, if the user passes on the software that circumvents the anti-copying measures, that would violate § 1201(b).<sup>73</sup>

#### 4. Exceptions for Anti-Circumvention Rules

The DMCA's anti-circumvention rules are subject to a set of specific exceptions,<sup>74</sup> which were the source of enormous controversy in the U.S. Congress.<sup>75</sup> This debate in Congress has been referred to as "a battle between Hollywood and Silicon Valley."<sup>76</sup> Hollywood and its allies,<sup>77</sup> representing the copyright industries, sought the strongest possible protection for the technological measures they used to protect their copyrighted works, while the Silicon Valley and its allies,<sup>78</sup> representing the information technology industries and the public user groups, opposed the expansive protections and argued that overbroad protection would bring deleterious effects "on their ability to engage in lawful reverse engineering, computer security testing, and encryption research."<sup>79</sup> It seems that Hollywood and its allies won this battle when they successfully persuaded Congress to pass the broad anti-circumvention rules. These rules are only subject to

<sup>72</sup> Singer, *supra* note 40, at 118. However, if the user uses this material in a very small area (e.g., in class) for purely educational or research purposes, he or she may have a fair use defense and may not be liable for copyright infringement. See 17 U.S.C. § 501.

<sup>73</sup> Singer provides a general example involving the eBook website. Singer, *supra* note 40, at 118–19.

<sup>74</sup> 17 U.S.C. § 1201(a)(1)(B), (c) (2002).

<sup>75</sup> "Congress sought a compromise that would keep the strong language of the statute but assuage the fears of some of the provision's opponents. This sought-after compromise ultimately led to a set of specific exceptions." See Hammond et al., *supra* note 47, at 597.

<sup>76</sup> Samuelson, *Anti-Circumvention*, *supra* note 43, at 522.

<sup>77</sup> Members of this group include the Motion Picture Association of America, Broadcast Music, Inc. (BMI), and the National Music Publishers Association, among others. See S. REP. NO. 105-190, at 3–4 (1998).

<sup>78</sup> Members of this group include the Digital Future Coalition, the Computer and Communications Industry Association, and the U.S. Activities Board Institute for Electrical and Electronics Engineers, among others. Broadly speaking, a coalition of public users, educators, librarians, and so forth (e.g. the U.S. National Commission on Libraries and Information Science), auguring for broader fair use exceptions, would also belong to the allies of Silicon Valley. *Id.* at 3–6.

<sup>79</sup> Samuelson, *Anti-Circumvention*, *supra* note 43, at 522–23.



some very specific exceptions that respond to some of concerns from Silicon Valley.<sup>80</sup>

a) Exceptions for § 1201(a)(1)(A)

Under the DMCA, the application of § 1201(a)(1)(A) (which bans the act of circumventing access controls) is subject to seven specific exceptions and one additional exception. The seven exceptions include:

- (1) *The nonprofit library, archive and educational institution exception* (§ 1201(d)). This exception allows nonprofit libraries, archives, and educational institutions to circumvent access-control measures solely for the purpose of making a good faith determination as to whether they wish to acquire authorized access to a protected work.<sup>81</sup>
- (2) *The governmental activities exception* (§ 1201(e)). This exception permits circumvention of access controls in the course of legitimate law enforcement, intelligence, and other governmental activities (such as national security activities) by governmental actors.<sup>82</sup>
- (3) *The reverse engineering exception* (§ 1201(f)). This exception allows circumvention of technical measures when necessary to achieve interoperability among computer programs. Specifically, it permits a person, who has lawfully obtained the rights to use a copy of a computer program,<sup>83</sup> to circumvent access controls for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability with other programs, to the extent that

<sup>80</sup> *Id.* at 523. However, these exceptions have been criticized as “confusing and somewhat contradictory.” *See, e.g.,* Burk, *supra* note 3, at 1104.

<sup>81</sup> 17 U.S.C. § 1201(d) (2002). However, it should be noted that “the exception does not apply where the institution can reasonably access the work in another manner, and even where applicable, the work may only be retained for a sufficient time to allow the institution to evaluate the work.” Bolinger, *supra* note 9, at 1096.

<sup>82</sup> 17 U.S.C. § 1201(e) (2002). *See also* Samuelson, *More Sensible Regulations*, *supra* note 51, at 3.

<sup>83</sup> As one commentator stated, despite the broad wording, the scope of applying this exception is still fairly narrow, because the exception applies solely to computer programs. Bolinger, *supra* note 9, at 1097.

such acts do not constitute infringement under copyright law.<sup>84</sup>

- (4) *The encryption research exception* (§ 1201(g)). This exception permits encryption researchers to circumvent access-control measures for the purpose of identifying flaws and vulnerabilities in encryption technologies.<sup>85</sup>
- (5) *The protection of minors exception* (§ 1201(h)). This exception allows users to circumvent technological prevention measure to prevent minors from accessing material on the Internet. Parents can use this exception to prevent their children from accessing harmful content on the Internet.<sup>86</sup>
- (6) *The personal privacy exception* (§ 1201(i)). This exception lets users circumvent access control measures when either the measures or the protected work collects or disseminates personally identifying information about the users' online activities.<sup>87</sup>
- (7) *The security testing exception* (§ 1201(j)). This exception permits users to circumvent access control measures to test the security of a computer, computer system, or computer network, as long as the owner or operator of the computer consents to the testing.<sup>88</sup>

In addition to the seven exceptions introduced above, the DMCA also provides a *basic exception for "classes of works."*<sup>89</sup> Sections 1201(a)(1)(B)–(E) establish an ongoing administrative rule-making process<sup>90</sup> and authorize the Librarian of Congress to periodically (every three years) exempt certain "classes of works"

---

<sup>84</sup> 17 U.S.C. § 1201(f) (2002). The statute defines the term "interoperability" as "the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged." 17 U.S.C. § 1201(f)(4).

<sup>85</sup> 17 U.S.C. § 1201(g) (2002).

<sup>86</sup> See Burk, *supra* note 3, at 1104.

<sup>87</sup> 17 U.S.C. § 1201(i) (2002). As one commentator stated, "Given the unfortunate trend of software distributors to include such capabilities in their works, this exception is necessary to protect the privacy of copyright users." Bolinger, *supra* note 9, at 1100.

<sup>88</sup> See COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 6.

<sup>89</sup> Lipton, *supra* note 11, at 343.

<sup>90</sup> See COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 5.

from the prohibition on access circumvention.<sup>91</sup> After extensive consultations, only two classes of works were exempted in the first round of rule making. They are:

- Compilations consisting of lists of websites blocked by filtering software applications;
- Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence.<sup>92</sup>

b) Exceptions for Anti-Devices Provisions: §§ 1201(a)(2) and 1201(b)

As limited as the exceptions to the anti-circumvention rule are, the exceptions to the anti-device rules are even narrower.<sup>93</sup> Only three of the seven specific exceptions discussed above apply to one or both of the anti-device rules.<sup>94</sup> Section 1201(f)(2) of the *reverse engineering* exception immunizes users from liability for circumventing access-control devices in § 1201(a)(2)) and rights-control devices in § 1201(b), when such circumvention is necessary for enabling interoperability among “computer programs.”<sup>95</sup> The *encryption research* (§ 1201(g)) and *security testing* (§1201(j)) exceptions are only available for the trafficking of the devices necessary to circumvent access-control measures (in § 1201(a)(2)); neither apply to the distribution the devices/tools necessary to circumvent rights-control measures (in § 1201(b)).<sup>96</sup>

c) Other General Provisions that Limit Anti-Circumvention Rules

The DMCA also contains general provisions limiting the scope of the anti-circumvention rules.<sup>97</sup> Section 1201(c) explicitly states that the anti-circumvention provisions in § 1201 are intended

---

<sup>91</sup> 17 U.S.C. § 1201(a)(1)(C) (2002).

<sup>92</sup> *Id.*

<sup>93</sup> See Hammond et al., *supra* note 47, at 596–97; see also Burk, *supra* note 3, at 1105.

<sup>94</sup> Samuelson, *More Sensible Regulations*, *supra* note 51, at Part IV.A.

<sup>95</sup> Burk, *supra* note 3; see 17 U.S.C. § 1201(f) (2002).

<sup>96</sup> Burk, *supra* note 3, at 1105; see 17 U.S.C. § 1201(g)(4), (j)(4) (2002).

<sup>97</sup> Samuelson, *More Sensible Regulations*, *supra* note 51, at Part IV.

neither to alter any rights, remedies, limitations, or defenses to copyright infringement, such as fair use under the Copyright Act,<sup>98</sup> nor “enlarge or diminish vicarious or contributory liability for copyright infringement.”<sup>99</sup> Section 1201(c) also provides that § 1201 would not oblige software and hardware manufacturers to design their products to accommodate “any particular technical measure used by those providing content for this equipment.”<sup>100</sup> Further, this limitation recognizes that some cases brought under the DMCA might raise First Amendment concerns,<sup>101</sup> and explicitly indicates that § 1201 would not “enlarge or diminish any rights of free speech or the press.”<sup>102</sup>

It is clear that, in enacting § 1201(c), Congress attempted to ameliorate the impact of the anti-circumvention rules on certain rights permitted by existing legislation (such as the right of fair use). However, it has not been entirely successful. A more in-depth discussion about the problems in the application of § 1201(c) (and its negative impacts on existing legal rights) follows below.<sup>103</sup>

## II. THE PROBLEMS WITH THE ANTI-CIRCUMVENTION RULES IN THE DMCA

Over the past few years, the DMCA and its anti-circumvention provisions in particular have been widely criticized. Pete Singer, Executive Editor of the 2002–2003 Dayton Law Journal, compiled a list of the adjectives used in ten different articles to criticize anti-circumvention provisions. He reported that:

---

<sup>98</sup> 17 U.S.C. § 1201(c)(1) (2002).

<sup>99</sup> *Id.* § 1201(c)(2) (2002).

<sup>100</sup> *Id.* § 1201(c)(3) (2002). It should be noted that, “despite this general ‘no mandate’ rule, § 1201(k) does mandate an affirmative response for one particular type of technology: within 18 months of enactment, all analog videocassette recorders must be designed to conform to certain defined technologies, commonly known as Macrovision, currently in use for preventing unauthorized copying of analog videocassettes and certain analog signals.” See COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 4; see also Samuelson, *Anti-Circumvention*, *supra* note 43, at 541.

<sup>101</sup> See Samuelson, *Anti-Circumvention*, *supra* note 43, at Part IV.

<sup>102</sup> 17 U.S.C. § 1201(c)(4) (2002).

<sup>103</sup> See *infra* notes 104–37 and accompanying text.

"Sucks," "evil," "wrongheaded," "much-hated," "unpredictable," "unsound," "ugly and inelegant," "inconsistent," "ill-conceived," "cumbersome," "overbroad," and "unconstitutional" are just a few of the adjectives that have been used to describe the anti-circumvention provisions of the Digital Millennium Copyright Act ("DMCA").<sup>104</sup>

This section will use recent cases and current examples to explore the major problems of the anti-circumvention provisions of the DMCA, investigate the main reasons for these problems, and examine how the rules work in practice.

*A. General Problems & Why There Is a Need for Anti-Device Rules*

The anti-circumvention provisions of the DMCA extend past the requirements of the WIPO Internet Treaties.<sup>105</sup> The DMCA not only prohibits the act of circumvention (which WIPO requires), but it also proscribes the manufacture and distribution of circumvention devices (the anti-devices rule, which WIPO does not require).<sup>106</sup> In response, some commentators argued that "copyright is moving ever further from controlling the existence of copies to controlling the use made of material, and dissemination of ideas, information, instruction and entertainment" and that this will make enforcement of § 1201 "increasingly problematic."<sup>107</sup>

It is not hard to understand why the U.S. Congress construed the anti-circumvention provisions in the WIPO Internet Treaties broadly and introduced the "anti-device" rules into the DMCA. Although copyright holders have started to apply technological measures to protect their works, technically sophisticated users can always find ways to circumvent or disable these technological

---

<sup>104</sup> See Singer, *supra* note 40, at 111.

<sup>105</sup> 17 U.S.C. § 1201 (a)(1)–(b) (2002); *see also supra* note 35.

<sup>106</sup> 17 U.S.C. § 1201 (a)(1)–(b).

<sup>107</sup> Cohen, *supra* note 33, at 981–82; *see also* Hector L. MacQueen, *Copyright and the Internet*, in *LAW & THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE* 222–23 (Lilian Edwards & Charlotte Waelde eds., Hart Publ'g 2000).

control measures.<sup>108</sup> They may even assist unsophisticated users in doing so, by supplying them with “user-friendly software ‘hacking tools.’”<sup>109</sup> The widespread availability of such tools or devices has greatly threatened the interests of copyright holders who employ technological protection measures on their works. The copyright industries realized the necessity of seeking legal support to prohibit circumvention activity, but litigation is time-consuming and expensive. Obviously suing individual users (circumventers) one-by-one is not a viable strategy for copyright holders. Although copyright holders (such as the music industries) could bring legal actions to some individuals, they could not sue each violator.<sup>110</sup> Therefore, to most effectively prevent the circumvention of technological protection measures and stop widespread piracy,<sup>111</sup> copyright holders must cut off circumvention at the source by limiting the availability of circumvention devices.

While § 1201 is vital to the copyright industries’ efforts to prevent circumvention activities, it arguably has broken the balance of interests between copyright holders and users under the

---

<sup>108</sup> See Schack, *supra* note 4, at 322.

<sup>109</sup> Burk, *supra* note 3, at 1102.

<sup>110</sup> The number of lawsuits filed by music industries is very limited/modest in comparison with the number of unauthorized music users. For example, in January 2004, the Recording Industry Association of America (RIAA) announced that it “filed a new round of copyright infringement lawsuits against 532 individual computer users who have been illegally distributing copyrighted music on peer-to-peer networks.” See *New Wave of Record Industry Lawsuits Brought Against 532 Illegal File Sharers*, at <http://www.riaa.com/news/newsletter/012104.asp> (Jan. 21, 2004). By contrast, before Napster failed its lawsuit, Napster announced that it had 20 million unique users by July 2000. See *Napster: 20 Million Users*, at <http://money.cnn.com/2000/07/19/technology/napster> (July 19, 2000).

<sup>111</sup> The Business Software Alliance (BSA) reported that 36% of the software in use worldwide was pirated in 2003, representing a loss of nearly US\$29 billion. See Press Release, Business Software Alliance, First Annual BSA and IDC Global Software Piracy Study (July 7, 2004) [hereinafter *BSA Study*], available at <http://www.bsa.org/usa-press/newsreleases/Major-Study-Finds-36-Percent-of-Software-in-Use-Worldwide-is-Pirated.cfm>. Moreover, according to research conducted by International Federation of the Phonographic Industry (IFPI), nearly 40% physical recordings in the market are illegal, and the value of the pirate market for music reached \$4.6 million in 2003. INTERNATIONAL ANTICOUNTERFEITING COALITION, THE NEGATIVE CONSEQUENCES OF INTERNATIONAL INTELLECTUAL PROPERTY THEFT: ECONOMIC HARM, THREATS TO THE PUBLIC HEALTH AND SAFETY, AND LINKS TO ORGANIZED CRIME AND TERRORIST ORGANIZATIONS 5 (2005), available at <http://www.iacc.org/WhitePaper.pdf> (last visited Apr. 2, 2005).

traditional copyright law.<sup>112</sup> Overly broad anti-circumvention rules, overly narrow exceptions (especially the exceptions for anti-device rules), and § 1201's structure put consumers and public users into a very weak position.<sup>113</sup> Another unexpected result of § 1201 is that many other groups with interests in preventing circumvention (apart from those seeking to protect copyrights), such as owners of confidential information, privacy-seeking individuals, and manufacturers who apply encryption technology in their products, became increasingly involved,<sup>114</sup> and further complicated the increasingly complex enforcement of anti-circumvention rules.<sup>115</sup> More details about these problems will be introduced in the next section.

*B. Problem I: Fair Use vs. Different Treatments in Anti-Circumvention Rules*

Although § 1201(c)(1) of the DMCA explicitly states "nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use" under the Copyright Act, this exception does not work effectively in practice.<sup>116</sup> The main reason may be that this exception is not equally applicable to the three anti-circumvention rules in the statute,<sup>117</sup> and § 1201 does not provide a general exception allowing users to circumvent access-control measures for the purposes of fair use.<sup>118</sup>

As to the application of the fair use rule in § 1201, the U.S. Copyright Office explicitly stated:

Since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumventing a technological measure that prevents copying [in § 1201(b)]. By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a

---

<sup>112</sup> See Cohen, *supra* note 33, at 985, 993.

<sup>113</sup> See *infra* Part II.B–C. See generally Singer, *supra* note 40.

<sup>114</sup> See Samuelson, *More Sensible Regulations*, *supra* note 51, at 7–8.

<sup>115</sup> *Id.*

<sup>116</sup> See Burk, *supra* note 3, at 1105.

<sup>117</sup> See Cohen, *supra* note 33, at 938.

<sup>118</sup> Burk, *supra* note 3, at 1105.

technological measure in order to gain access [in § 1201(a)(2)] is prohibited.<sup>119</sup>

According to this explanation, the fair use defense seems only to allow users who already have lawful access to a work to circumvent a technological measure which protects rights controls. One example of the application of the U.S. Copyright Office explanation can be found in *Universal City Studios v. Corley* (“*Corley*”).<sup>120</sup> In that case, Universal City Studios enlisted the help of the DVD Copy Control Association, which is responsible for licensing encryption technology called the Content Scramble System (“CSS”), to prevent unauthorized copying of Digital Video Disc (“DVD”) movies.<sup>121</sup> Jon Johansen, a Norwegian teenage programmer developed CSS decryption software (a program called DeCSS), which can be used to circumvent CSS and disable the encryption mechanism contained in DVDs.<sup>122</sup> Corley posted DeCSS on his magazine’s website, 2600.com, and made it freely downloadable to all subscribers.<sup>123</sup> In response, Universal City Studios brought an action against Corley claiming a violation of § 1201(a)(2).<sup>124</sup> Although Congress intended to treat access controls differently from copy controls “on the theory that lawful access was a prerequisite for fair use rights,”<sup>125</sup> the court treated CSS as an access-control measure nonetheless, and agreed with Universal City Studios’ arguments.<sup>126</sup> Consequently, as Professor Samuelson stated, “[b]y ruling that *DeCSS* was a 1201(a)(2) tool, not a 1201(b)(1) tool, the court implicitly ruled that circumventing CSS [(i.e., circumventing an access-control measure in § 1201(a)(2))] to make fair use of a DVD movie violates 1201(a)(1)(A).”<sup>127</sup>

---

<sup>119</sup> COPYRIGHT OFFICE DMCA SUMMARY, *supra* note 24, at 3–4.

<sup>120</sup> 273 F.3d 429 (2d Cir. 2001).

<sup>121</sup> *Id.* at 436.

<sup>122</sup> See, e.g., Press Release, Elec. Frontier Found., California Supreme Court to Hear DVD Case: Publication of DVD Decryption Information Is Constitutional (May 27, 2003), at [http://www EFF.org/IP/Video/DVDCCA\\_case/20030527\\_bunner\\_supreme-court\\_pr.php](http://www EFF.org/IP/Video/DVDCCA_case/20030527_bunner_supreme-court_pr.php).

<sup>123</sup> See *Corley*, 273 F.3d at 435–36.

<sup>124</sup> *Id.* at 436.

<sup>125</sup> See Samuelson, *DRM*, *supra* note 13, at 42.

<sup>126</sup> *Corley*, 273 F.3d at 436; see also Samuelson, *DRM*, *supra* note 13, at 42.

<sup>127</sup> See Samuelson, *DRM*, *supra* note 13, at 43.



The court correctly applied the explanation the U.S. Copyright Office made regarding the application of the fair use rule in § 1201,<sup>128</sup> and the court's reasoning (and decision) was correct. Nevertheless, the result is undesirable: if a user circumvents access control measures, even for fair use, the user will still be found to violate § 1201(a)(1)(A).<sup>129</sup> Thus, it seems that "fair access" has become a prerequisite of making fair use. Therefore, under § 1201, the application of the fair use doctrine may be summarized as: "Fair Use = Fair Circumvention on Access Controls + Fair Circumvention on Right Controls."

In addition, Nimmer provides a summary about the practical effects of implementing § 1201. He states:

As to prohibited access, the person engaging in that conduct has violated the basic provision [in § 1201(a)(1)(A)]; anyone assisting her through publicly offering services, products, devices . . . to achieve the prohibited technological breach is separately culpable under the ban on trafficking [in § 1201(a)(2)]. By contrast, a person who engaged in prohibited usage of a work to which he has lawful access does not run afoul of any provision of section 1201. It is only someone who assists him through publicly offering services, products, devices, etc., to achieve the prohibited technological breach who becomes culpable under the additional violations [§ 1201(b)].<sup>130</sup>

Under this interpretation of the law, two issues arise. First, how could a person make fair use of a work when it is illegal for her to gain access to the work? Second, even if a user has lawful access, she may still not be able to make fair use of a copyrighted work if she does not have enough decryption knowledge to hack through the protection measure. Although a user is not liable for

<sup>128</sup> See *supra* notes 118–19 and accompanying text.

<sup>129</sup> See Press Release, Congresswoman Zoe Lofgren, Section by Section Analysis of "The Digital Choice and Freedom Act of 2002," at [http://www.house.gov/lofgren/news/2002/021002\\_detail.htm](http://www.house.gov/lofgren/news/2002/021002_detail.htm) (last visited Apr. 2, 2005) ("Contrary to the intent of Congress, section 1201 of the DMCA has been used to prohibit lawful users from circumventing technical restrictions for any reason, even to pursue their fair use rights.").

<sup>130</sup> See Nimmer, *supra* note 65, at 689.

circumventing post-access control/rights control technological measures under § 1201,<sup>131</sup> the person who assists the user by publicly offering services or devices to circumvent the technology will violate § 1201(b).<sup>132</sup> Thus, if users cannot circumvent the right control measures by themselves, it may be very hard to find a person to assist them. Even if the user has the relevant skills to circumvent the protection measures, she may still not be able to do so because most circumvention devices have been banned by the anti-device provisions of § 1201 and are no longer available for public use.<sup>133</sup> As one commentator stated, “without the necessary tools and knowledge, normal users are left helpless.”<sup>134</sup>

*C. Problem II: Overly Narrow Exceptions & Lack of a General Purpose Exception for Other Legitimate Reasons*

Although the DMCA was not intended to alter user privileges (including fair use) established by traditional copyright law,<sup>135</sup> overly narrow exceptions compromise this aim, to the detriment of copyright content users and, in some circumstances, copyright owners.

Anti-circumvention rules frustrate users who wish to make legitimate fair use of copyrighted content. Due to the lack of a

---

<sup>131</sup> As the U.S. Copyright Office stated, “since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumventing a technological measure that prevents copying [in § 1201(b)].” See *supra* notes 118–19 and accompanying text; see also *supra* notes 66–73 and accompanying text (“AGLC” e-book example). Assume a law professor wants to print out a 1-2 page handout from the AGLC e-book for her students, but she does not have enough skills to circumvent rights-control measures that prevent users from printing PDF documents in the AGLC website. As a result, the professor has a computer programmer help her breach the rights-control measures and they print out the AGLC PDF document. In this hypothetical, the professor would not be liable for the § 1201(b) violation, but the programmer would be.

<sup>132</sup> See Nimmer, *supra* note 65, at 689.

<sup>133</sup> 17 U.S.C. § 1201(a)(1) (2002). Again, the AGLC e-book provides a useful example. See *supra* notes 66–73, 131–32 and accompanying text. Assume a law professor has the skill to circumvent rights-control measures that prevent users from printing PDF documents from the AGLC website. Even so, she still may not be able to circumvent them because most circumvention devices (such as decryption software) have been banned by the anti-device provision of § 1201(b), and the relevant tools or software are not available on the market.

<sup>134</sup> Schack, *supra* note 4, at 327.

<sup>135</sup> 17 U.S.C. § 1201(c)(1)–(4) (2002).

general exception for fair use circumvention of access-control measures, even if a user has the right to make fair use of a protected work, she still may not be able to use it.<sup>136</sup> In addition, the anti-circumvention rule provides protections for all protected elements, regardless of whether they include un-copyrightable facts, public domain materials, or purely functional works.<sup>137</sup> Unauthorized extraction of these elements does not violate copyright,<sup>138</sup> yet extraction of such uncopyrightable content from a technologically protected copy may constitute a violation of anti-circumvention rules of the current DMCA.<sup>139</sup> This threatens users' rights on using uncopyrightable materials, especially materials in the public domain.

Anti-circumvention rules may also threaten the rights granted to copyright holders. For example, if a copyright owner wants to detect whether an infringing copy of his original work has been included in an encrypted database website (e.g., an online research paper database), he may have to circumvent the suspected infringer's access control measures. However, even if unauthorized copyright materials are found in the database, the copyright owner still has violated § 1201(a)(1)(A) because he circumvented the access-control measure during his investigation.<sup>140</sup> Other possible situations where circumvention of access controls may be necessary include: detecting a highly destructive computer virus or worm in an encrypted digital object, conducting a computer security test without permission of either the owner or manufacturer of such systems, or detecting information in encrypted floppy disks for the purpose of free press and free speech interests.<sup>141</sup> In order to protect the benefits to different parties and to sustain the fair use doctrine, Congress needs a more general "other legitimate purposes" exception to enable users to circumvent access-control measures when

---

<sup>136</sup> See *supra* notes 90–92 and accompanying text.

<sup>137</sup> See Burk, *supra* note 3, at 1108.

<sup>138</sup> See *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340 (1991).

<sup>139</sup> See, e.g., Burk, *supra* note 3, at 1108.

<sup>140</sup> See Samuelson, *Anti-Circumvention*, *supra* note 43, at 543 (providing a similar example).

<sup>141</sup> *Id.* at 543–46.

circumvention may be necessary for certain purposes but is not authorized by existing exceptions in § 1201.<sup>142</sup>

*D. Problem III: “Para-Copyright” Provisions & Misuse of Anti-Circumvention Rights*

Many commentators argue that the anti-circumvention provisions of the DMCA enable a new form of exclusive right for content owner: a right of access.<sup>143</sup> This right not only facilitates the licensing of copyrighted materials, but also allows licensing of access to uncopyrighted materials.<sup>144</sup> Although anti-circumvention provisions are part of the DMCA, and are frequently mentioned in connection with copyright, they are entirely separate from exclusive rights provisions under traditional copyright law,<sup>145</sup> and a technological infringer does not need to infringe any of the exclusive rights of copyright holders to violate § 1201.<sup>146</sup> Thus, some commentators dub the anti-circumvention rights under the § 1201 as “para-copyright.”<sup>147</sup>

The copyright industry is no longer the sole entity using technical measures to protect their digital information.<sup>148</sup> Trade secret owners, privacy-seeking individuals, and others possessing confidential information also started to apply technical protection measures to “protect their legitimate interests in digital information.”<sup>149</sup> In *Lexmark Int’l, Inc. v. Static Control*

<sup>142</sup> See Hammond et al., *supra* note 47, at 599; Samuelson, *Anti-Circumvention*, *supra* note 43, at 519, 543.

<sup>143</sup> Burk, *supra* note 3, at 1106; see also Ginsburg, *Copyright Legislation*, *supra* note 65, at 140–43. Ginsburg argued that the DMCA creates a new ‘right of access.’

<sup>144</sup> Burk, *supra* note 3, at 1109; see also Schack, *supra* note 4, at 324 (stating that “this legal protection of anti-circumvention measures as such permits proprietary control over any kind of information, protected or not under copyright.”).

<sup>145</sup> Burk, *supra* note 3, at 1106–07.

<sup>146</sup> *Id.* A violation of exclusive rights of copyright holders under traditional copyright law is not a prerequisite for a violation of the anti-circumvention provision. The applications of anti-circumvention rules (anti-devices rules in particular) have gone much further than the scope of copyright and requirements of WIPO Internet Treaties. See *supra* notes 25–30 and accompanying text. They have threatened the permitted privileges of users (such as fair use) under traditional copyright law. See *supra* notes 112–42 and accompanying text.

<sup>147</sup> Schack, *supra* note 4, at 324; see also Burk, *supra* note 3, at 1095.

<sup>148</sup> Ginsburg, *Copyright Legislation*, *supra* note 65, at 178–79.

<sup>149</sup> Samuelson, *More Sensible Regulations*, *supra* note 51, at 7.

*Components, Inc.*,<sup>150</sup> Lexmark brought an action against a manufacturer of computer chips, Static Control Components (SCC), claiming circumvention infringement under the DMCA.<sup>151</sup> Lexmark, a major manufacturer of printers and ink toner cartridges, applied a special technological protection measure to the chips of its cartridges.<sup>152</sup> This technological measure not only prevented rival manufacturers' cartridges from being recognized by Lexmark's printers, but also prevented refilled aftermarket Lexmark cartridges from functioning with Lexmark's printers.<sup>153</sup> Lexmark claimed that by providing chips that enable rival cartridges to be recognized by Lexmark's printer, Static Control Components violated § 1201(a)(2) of the DMCA by trafficking in a device which circumvents a technological protection measure.<sup>154</sup>

Because this claim has nothing to do with the infringement of copyrighted content, one commentator criticized "it is a fairly naked attempt to suppress competition in the market for printer ink cartridges."<sup>155</sup> Although the U.S. Court of Appeals for the Sixth Circuit finally ruled favorably in SCC's appeal on the preliminary injunction,<sup>156</sup> the court "has not established the effect of this ruling on other aftermarket chips."<sup>157</sup>

---

<sup>150</sup> 387 F.3d 522 (6th Cir. 2004).

<sup>151</sup> *Id.* at 528–29.

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> Burk, *supra* note 3, at 1110. Moreover, it should be noted that a bill was passed, effective Oct. 1, 2003, "that will allow printer users the right to refill any cartridge, voiding contracts or purchase agreements that ban cartridges from being remanufactured. . . . 'This act becomes effective October 1, 2003, and applies to agreements or contracts entered into on or after that date. This act does not apply to or affect any litigation pending before that date.'" See *N.C. Bill Signed by Governor; Makes Cartridge Return Agreements Unenforceable*, at <http://www.rechargermag.com/news.asp?id=200308502> (Aug. 11, 2003).

<sup>156</sup> See *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004); see also Press Release, Charles Taylor, Director of Media Relations, Static Control Components, Inc., Sixth Circuit Rules in Favor of Static Control Components (Oct. 26, 2004), at [http://www.scc-inc.com/ScCVsLexmark/pdf\\_lawsuit/Circuit-RulingSCCPressRelease.pdf](http://www.scc-inc.com/ScCVsLexmark/pdf_lawsuit/Circuit-RulingSCCPressRelease.pdf).

<sup>157</sup> See *Static Control Components, Inc., SCC vs. Lexmark*, at <http://www.scc-inc.com/ScCVsLexmark> (last visited Apr. 2, 2005) ("SCC's customers do not need to be concerned with copyright or Digital Millennium Copyright Act Issues. [But] [t]he court has not established the effect of this ruling on other aftermarket chips.").

The battle turned from printer toner cartridges to garage door openers in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*<sup>158</sup> Chamberlain is a manufacturer of garage door opener systems. These systems use a rolling code (a computer program) that prevents any capturing and recording of transmitter signals, thereby preventing burglars from gaining access to a homeowner's garage.<sup>159</sup> Skylink, a competitor of Chamberlain, distributed a universal remote control device that enables consumers to operate different brands of garage door openers, including Chamberlain's.<sup>160</sup> Chamberlain filed a lawsuit against Skylink for violating the anti-trafficking provision in § 1201(a)(2) of DMCA.<sup>161</sup> It claimed that Skylink and homeowners circumvented Chamberlain's "security measure in the rolling code" without authorizations.<sup>162</sup> The district court dismissed Chamberlain's claim,<sup>163</sup> finding that "this did not establish that Skylink violated the DMCA, and to the extent the competitor was authorized [to] reverse-engineer the manufacturer's openers, it could not have been held liable under the DMCA,"<sup>164</sup> The court's ruling arguably puts certain "limits on the power of the anti-circumvention

<sup>158</sup> *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003), *aff'd*, 381 F.3d 1178 (Fed. Cir. 2004).

<sup>159</sup> Unlike other garage door openers, which use a fixed code and a burglar can record by using a code grabber, Chamberlain's technology could effectively prevent the use of code grabbers because a previously used code will not be recognized by Chamberlain's system. See James D. Nguyen, *Code Breaking: The DMCA Provides a Powerful Tool for Content Owners to Thwart the Circumvention of Antipiracy Technology*, 27 L.A. LAW. 33, 40 (May 2004).

<sup>160</sup> *Id.*

<sup>161</sup> Chamberlain claimed Skylink's opener violated Section 1201(a)(2) "because 1) the opener was primarily designed to circumvent Chamberlain's system, 2) it has a limited commercial purpose other than to circumvent the system, and 3) it is marketed to circumvent the system." *Id.* at 40.

<sup>162</sup> See Molly Torsen, *Lexmark, Watermarks, Skylink and Marketplaces: Misuse and Misperception of the Digital Millennium Copyright Act's Anticircumvention Provision*, 4 CHI.-KENT J. INTELL. PROP. 117 (2004).

<sup>163</sup> *Chamberlain*, 292 F. Supp. 2d at 1046 (N.D. Ill. 2003), *aff'd*, 381 F.3d 1178 (Fed. Cir. 2004).

<sup>164</sup> Torsen, *supra* note 162; see also *Chamberlain*, 292 F. Supp. 2d at 1044-45 ("In any event, regardless of which party bears the burden of proof on this issue, it is clear that to the extent Skylink was authorized to decrypt, descramble, avoid, bypass, remove, deactivate, or impair Chamberlain's GDOs, it cannot be held liable under the DMCA. . . . [A] homeowner has a legitimate expectation that he or she will be able to access the garage even if the original transmitter is misplaced or malfunctions.").

provisions,”<sup>165</sup> and as a result will help prevent misuses of anti-circumvention rules and “encourage free market competition” between different door opener manufacturers.<sup>166</sup> Nevertheless, the court’s decision does not guarantee similar misuses would not happen in other industries or jurisdictions in the future.

Another example is *RealNetworks, Inc. v. Streambox, Inc.*,<sup>167</sup> in which the defendant, Streambox, was charged with contributory copyright infringement and violation of § 1201(b) of the DMCA. The plaintiff, RealNetworks, develops and markets software products designed to enable owners of audio, video, and other multimedia content to send their content, by “streaming,” to users of personal computers over the Internet.<sup>168</sup> RealNetworks claimed that Streambox distributed and marketed products that would bypass technological control measures established by RealNetworks (called a “Secret Handshake” protocol),<sup>169</sup> and enable users to make unauthorized copies of files and convert those files into other formats.<sup>170</sup> After a detailed investigation, the court found that the program “Streambox VCR,” designed by Streambox, was primarily used for circumventing RealNetworks’ access-control and copy-control measures,<sup>171</sup> and the program “Ferret” was mainly designed to create unauthorized derivatives of

---

<sup>165</sup> See Nguyen, *supra* note 159, at 40.

<sup>166</sup> See Torsen, *supra* note 161.

<sup>167</sup> No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

<sup>168</sup> See *id.* at \*\*1–2.

<sup>169</sup> RealNetworks applied a special technological measure (“Secret Handshake”) to its software products which allow the server and receiver to recognize one another. Once a connection is established, the Secret Handshake will enable the system to automatically determine whether the receiver’s user has been authorized to reproduce the music files sent by the server, or only has right to listen. *Id.*

<sup>170</sup> Eleanor M. Lackman, *Slowing Down the Speed of Sound: A Transatlantic Race to Head off Digital Copyright Infringement*, 13 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1161, 1172 (2003).

<sup>171</sup> *RealNetworks*, 2000 WL 127311, at \*8. The program “Streambox VCR” (developed by Streambox) is designed to be interoperable with the RealPlayer system. Once the program is installed, it would imitate RealNetworks’ Secret Handshake. Thus RealNetworks’ program would think the user of the Streambox VCR had been authorized to download and copy files. See Lackman, *supra* note 170, at 1172 n.76.

copyrighted works in formats other than plaintiff's program.<sup>172</sup> Thus, the court granted preliminary injunctions on RealNetwork's claims that Streambox VCR violated § 1201(b)<sup>173</sup> and Ferret constituted a contributory copyright infringement.<sup>174</sup> In this case, like the *Chamberlain* case, only producers of competing software technology were involved, but here the court ruled there was a DMCA violation because the technology protected copyrighted content.

As demonstrated above, plaintiffs have begun testing § 1201 of the DMCA, even in non-copyright situations. Such attempts could increase the risk of the misuse of anti-circumvention rules in non-copyright industries, and encourage conflicts between anti-circumvention rights and rights which have been established under other legislation, like traditional copyright law or competition law.<sup>175</sup> Although most decisions that courts have made so far are in favor of protecting free competition and limiting the misuse of anti-circumvention rules, these decisions could not guarantee similar misuses would not happen in other industries or jurisdictions in the future (as introduced above).<sup>176</sup> Thus, in order to solve problems inherent in anti-circumvention rules,<sup>177</sup> to reduce the risk of misusing copyright law, and to enhance consumer protections and free market competition, it has become increasingly necessary to modify anti-circumvention provision rules in the current DMCA and to limit the rights of those who apply technological protection measures to their products.

---

<sup>172</sup> See Lackman, *supra* note 170, at 1172 n.76. Once the "Ferret" is installed as a "plug-in" to a user's computer, it will enable a user to alter the visual appearance and operation of RealNetworks' interface. *RealNetworks*, 2000 WL 127311, at \*\*6, 12.

<sup>173</sup> *RealNetworks*, 2000 WL 127311, at \*\*7–11.

<sup>174</sup> *Id.* at \*\*11–12; see also Eddan Elizafon Katz, *RealNetworks, Inc. v. Streambox, Inc. & Universal City Studios, Inc. v. Reimerdes*, 16 BERKELEY TECH. L.J. 53, 58 (2001).

<sup>175</sup> See *supra* notes 143–74 and accompanying text.

<sup>176</sup> *Id.*

<sup>177</sup> See *supra* notes 112–42 and accompanying text.



### III. FUTURE ANTI-CIRCUMVENTION RULES: HETEROGENEOUS SOLUTIONS

Part III will suggest some specific solutions to the main problems with the current anti-circumvention rules examined above. It will draw on experiences from current domestic legislation, such as the “notice and takedown regime” in the DMCA Internet Service Provider (“ISP”) Safe Harbor provisions and relevant provisions in the proposed Digital Choice and Freedom Act, as well as legislation in other countries, particularly Germany. It will argue for establishing a “fair circumvention” doctrine. This section will also propose that the best way to solve the problems of the DMCA anti-circumvention provisions is to use a more heterogeneous method and amend current copyright statutes. It argues that the best solution lies in increasing courts’ discretion on certain issues, establishing necessary government agencies, and applying the power of the market.

#### A. *Broader Exceptions: Fair Circumvention Doctrine (A Statutory/Common Law Solution)*

Copyright law should ensure that consumers and public users have easy access to online materials and that unreasonable burdens are not imposed on the technology, while simultaneously providing the copyright industries with enough incentive to continue creating new works.<sup>178</sup> The same holds true for anti-circumvention provisions.<sup>179</sup> Overly narrow exceptions to § 1201 will not achieve such a balance. It seems increasingly necessary to adopt broader exceptions to § 1201 to facilitate legitimate users’ exercise of rights, such as fair use, that are permitted by traditional copyright law. Generally, in order to make fair use of a technologically-protected copyrighted work, a user must first successfully circumvent both access-control measures and right-control measures that copyright holders employ on these works.<sup>180</sup> However, although § 1201 permits a user to circumvent post-

---

<sup>178</sup> Newton, *supra* note 2, at 127.

<sup>179</sup> Samuelson, *Anti-Circumvention*, *supra* note 43, at 519.

<sup>180</sup> June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM.-VLA J.L. & ARTS 385, 393–94 (2004).

access rights-control measures for fair use purposes, the user will still violate § 1201(a)(1)(A) if he circumvents the access-control measures without authorization.<sup>181</sup>

A “fair circumvention” doctrine will provide the necessary “catchall” exception for all other legitimate purposes. For clarity, this should include an explicit exception enabling users to lawfully circumvent all technological protection measures, including both access-control and rights-control measures, in order to make fair use of the technologically-protected works. Under this proposed doctrine, if a user has the privilege to make fair use of an article in an online database, then he will automatically have a privilege to circumvent any technical measures that would prevent him from legitimately using this article. Here, in order to make a fair use, a user could circumvent the password page, an access-control measure, and reactivate the disabled print button, a rights-control measure.

Future changes to the DMCA can include a broader wording of the fair circumvention exception, an example of which can be found in the U.S.’s Digital Media Consumers’ Rights Act.<sup>182</sup> This bill, which the House Subcommittee on Commerce, Trade and Consumer Protection is currently considering, provides that “circumvention would be lawful as long as it does not result in copyright infringement.”<sup>183</sup> It also permits users to manufacture and distribute circumvention devices and technologies that would “enable significant non-infringing uses of copyrighted works.”<sup>184</sup> Similar provisions may be added to the DMCA.

However, in order to prevent an overly broad exception for fair circumvention, future additions to the DMCA should also include specific conditions and circumstances to limit the applicability of this exception. In this respect, the U.S.’s proposed Digital Choice and Freedom Act (“DCFA”) may serve as a good template.<sup>185</sup> Under the DCFA, a user would be allowed to circumvent technical

---

<sup>181</sup> See *supra* Part III.E.2.

<sup>182</sup> Digital Media Consumers’ Rights Act of 2003, H.R. 107, 108th Cong.

<sup>183</sup> Samuelson, *DRM*, *supra* note 13, at 45.

<sup>184</sup> *Id.* These exceptions not only enable users to exercise fair use rights, but also enable them to conduct all non-infringing uses of copyright works.

<sup>185</sup> Digital Choice and Freedom Act of 2002, H.R. 6932, 107th Cong. (2002).

measures to make non-infringing use of a work only “if the copyright owner has not made publicly available the necessary means to permit the noninfringing uses without additional cost or burden to users.”<sup>186</sup> Nevertheless, it would be better if future laws gave courts the discretion to decide, case-by-case, if the fair circumvention exception applies. As Samuelson stated, “[i]n many other parts of copyright law—the fair use doctrine, for example—Congress has trusted the courts to employ a situationally-based analysis to distinguish between legitimate and illegitimate activities. It should have done so with respect to the anti-circumvention rules as well.”<sup>187</sup> In short, future laws should provide more leeway for consumers and public users to use online materials, but this leeway should be a limited privilege.

The 2001 E.C. Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society (“Information Society Directive”) adopted a unique approach to the aforementioned DMCA provisions.<sup>188</sup> In Article 6, paragraph 4, the directive tries to reconcile protecting effective anti-circumvention measures with limiting copyright protections to allow users to use the materials.<sup>189</sup> Specifically, it proposes two ways to achieve such a purpose.<sup>190</sup> First, the directive relies on voluntary measures taken by the copyright holders to ensure the users’ fair use rights.<sup>191</sup> Second, in the absence of voluntary measures, the directive requires the member countries to take “appropriate measures” to ensure that copyright holders make available to the public “the means of benefiting from that exception or limitation.”<sup>192</sup>

Although the proposed solutions are far from perfect, the E.U. legislation evidences a greater awareness than the DMCA of the

---

<sup>186</sup> Samuelson, *DRM*, *supra* note 13, at 45.

<sup>187</sup> Samuelson, *More Sensible Regulations*, *supra* note 51, at 6–7.

<sup>188</sup> Council Directive 2001/29/EC, 2001 O.J. (L 167) 10 [hereinafter Information Society Directive].

<sup>189</sup> Anti-circumvention measures are required according to paragraph 1 of the Information Society Directive. *See id.*, art. 6, ¶ 1; Schack, *supra* note 4, at 324.

<sup>190</sup> *See* Information Society Directive, *supra* note 188, art. 6, ¶ 4.

<sup>191</sup> *See id.* (including agreements between copyright holders and other parties concerned).

<sup>192</sup> *See id.*

problem of preserving the fair use rights of public users.<sup>193</sup> The DMCA should be amended to encourage voluntary measures, or to directly provide specific measures to enhance the enforcement of fair use doctrine.<sup>194</sup>

*B. Controlling Technological Measures to Protect Users:  
Proposed Legal Solutions & Market Solutions*

Strong legal protection for technological protection measures obviously favors copyright holders, and may be abused to limit competition or consumer rights.<sup>195</sup> When those protections have been passed, it is necessary to also strengthen the controls on technological protection measures so that the measures will not be overused to the detriment of consumers and the public. Amendments to the DMCA could establish a general principle for strengthening the control of technological protection measures by providing that (i) technical protection measures must accommodate rights that have been established by existing legislation, including permitted privileges in traditional copyright law, and (ii) if a technical protection measure eliminates those privileges, then it will lose legal protection and all users may legally circumvent it. Moreover, since the technological protection measures have been used in many non-copyright situations and have obviously exceeded the scope of traditional copyright law, future legislation should also give the courts discretion to decide whether a specific technological protection measure conflicts with existing legislation or competition law.

In addition, future legislation may also establish specific legal mechanisms to facilitate the enforcement of such control. It may be necessary to appoint a special governmental agency, or a special work group within the U.S. Copyright Office, to deal with all of

---

<sup>193</sup> See Schack, *supra* note 4, at 325–26. However, the directive does not provide any specific explanation of “appropriate measures.” Schack criticized, “As the EU did not know how to square the circle of protecting anti-circumvention measures and fair use at the same time, it hopes that the Member States will find the solution.” *Id.* at 325.

<sup>194</sup> Specific suggestions on appropriate measures (legal mechanisms) will be introduced in the next sections. See *infra* Parts IV.B–C.

<sup>195</sup> See *supra* Part III.E.4.

the issues relating to technological protection measures. The major objectives of this agency should include:

- (1) Strengthening control on Technological Protection Measures (TPM),
- (2) Providing circumvention assistance to eligible users seeking to exercise their rights,
- (3) Balancing benefits between public users and copyright holders,
- (4) Facilitating evidence collection, and
- (5) Relieving the burden of courts on TPM issues.

In the proposed system, copyright holders who employ technological protection measures on their works would be encouraged to register their technological measures with the appointed government agency, perhaps initially on a voluntary basis (a “soft law” approach). The copyright holders would complete a formatted registration form, on which they would include their contact information, the main purpose of their technological protection measures, the application scope of their technological protection measures, and other relevant information.<sup>196</sup> They would also be encouraged to deposit a “key” of their technological measures, in the form of a temporal password or decryption method, to the neutral government agency in order to facilitate possible fair circumvention activities in the future. If required, the agency may also evaluate their registration materials and decide whether their technological protection measures or application of this measure are lawful, and if so, issue a certificate to confirm their validity. A *prima facie* conclusion of validity of a technological protection measure should be made on the basis of submitted formatted application materials and a preliminary examination/evaluation of whether the application of

---

<sup>196</sup> An analogous approach can be found in the counterpart of “Notice and Takedown” in the DMCA. In that regime, in order to lodge an effective takedown notice, the aggrieved party (i.e. copyright holder) is required to submit a formal notice to the ISP’s agent. *See* 17 U.S.C. § 512(c)(3). Takedown notice is necessary for the copyright holder to establish the ISP’s requisite knowledge for liability. *Id.* Effective notice contains six specific identifying elements, such as the signature of a person authorized to act on behalf of the owner of the allegedly infringed copyright. *Id.*

such technological measure would conflict with existing legislation.<sup>197</sup> In addition, the certificate of validity could serve as important evidence in future court litigation.

Amendments should also establish a legal mechanism to enhance the involvement of consumers and apply market forces to solve these problems. The Information Society Directive provides some insight into how the market can be used to correct anti-circumvention issues.<sup>198</sup> In order to implement the Information Society Directive, § 95d(1) of a German bill from July 21, 2002 included a provision requiring that “all goods protected by technological measures must be marked with clearly visible information about the properties of the technological measures.”<sup>199</sup> By requiring notification of technological protection measures on products, the German consumers will have an opportunity to choose between a product not containing any technological protection measures and a product with those measures, such as CDs that cannot be played on a personal computer. Similar provisions may be added to the DMCA in order to enhance the involvement of American consumers.<sup>200</sup>

---

<sup>197</sup> For example, the government agency may hold a technical measure is unlawful, if the application of the technical measure would directly destroy the computer hard disk of any user who intends to circumvent such technical measure (such as by releasing computer viruses), and/or would seriously threaten the security of Internet.

<sup>198</sup> See Information Society Directive, *supra* note 188.

<sup>199</sup> Schack, *supra* note 4, at 332; see also Information Society Directive, *supra* note 188.

<sup>200</sup> A similar proposal could also be found in the Digital Media Consumers' Rights Act of 2002 (DMCRA). See H.R. 5544, 107th Cong. (2002). In order to strengthen the protection to consumers, the DMCRA tried to “reduce the heavy handed tactics of recording companies by making them disclose when CDs they produce utilize copy protection technology.” See Kevin C. Earle, Comment, *No-Copy Technology and the Copyright Act: Has the Music Industry Been Allowed to Go Too Far in Diminishing the Consumers' Personal Use Rights in the Digital World?*, 2 J. MARSHALL REV. INTELL. PROP. L. 337, 358 (2003), at <http://www.jmls.edu/ripl/vol2/issue2/earle.pdf>. Specifically, § 3 of the DMCRA established “the new labeling and enforcement requirements with respect to these new, non-standard ‘copy protected compact discs.’” For more details, see *Digital Media Consumers' Rights Act Section-by-Section Description*, at <http://www.house.gov/boucher/docs/dmcrasec.htm>.

*C. Predictable Problems on Enforcement of New Doctrine & Possible Legal Solutions*

Even if a broad fair circumvention doctrine and a strong legal control on technology protection measures are established, enforcement may still be very problematic. At least two major problems arise. First, even if a user has the right to circumvent technological protection measures, she may not be able to exercise this right. As discussed before, a lawful user may not be able to circumvent the technological measures simply because the user does not have enough decryption skills.<sup>201</sup> Even if the user has those skills, she may be thwarted because devices have been banned by § 1201 and are not available for her to use.<sup>202</sup> An amended DMCA should also explicitly provide that the fair circumvention doctrine is not only applicable to § 1201(a)(1)(A) (which would allow the user to circumvent the access-control measures), but also to the anti-devices rules in § 1201(a)(2) and (b). This would allow people to make, traffic in, and distribute the technologies and devices enabling non-infringing uses of copyrighted works, as suggested by the Digital Media Consumers' Rights Bill.<sup>203</sup> Otherwise, "even where circumvention itself might be legal, the vast majority of users would be deprived of the devices and expert help needed to exercise their rights."<sup>204</sup>

To enforce the fair circumvention doctrine, a future DMCA amendment should provide specific legal mechanisms to help eligible users obtain necessary circumvention assistance from the appointed government agency when these users are not capable of circumventing the technological protection measures by themselves. The amended DMCA may draw on experiences from the "notice and takedown regime" in the ISP Safe Harbor provisions,<sup>205</sup> and set up a specific "fair circumvention application procedure." Under the new procedures, a user should first lodge a formal application for assistance. Then, the agency will assess the application and decide whether the user is eligible for their

---

<sup>201</sup> See *supra* Part III.E.2.

<sup>202</sup> *Id.*

<sup>203</sup> See *supra* notes 144–77.

<sup>204</sup> Schack, *supra* note 4, at 325.

<sup>205</sup> 17 U.S.C. § 512 (2002).

assistance. Once the user is considered eligible, the agency will assist the user in circumventing the protection measures, perhaps by providing a temporary password to users. If the agency is not capable of circumventing the technological measures, perhaps because the copyright holder did not register the technological protection measure, then the agency should work with the court to require the copyright holders to provide assistance, or with agents of the copyright holders specifically designated for this purpose.

The second problem is that the fair circumvention doctrine may be abused by users to harm the copyright holders. This Article posits that copyright law should keep a neutral position when balancing the benefits of public users and copyright holders, and not favor either position. Again, this aim could be achieved by establishing some specific legal procedures. Based on the fair circumvention application procedures proposed above, legislators can go further and provide additional specific requirements. For example, the new procedure could require users to fill in a formatted application form and to submit it to the relevant government agency, or court, before conducting a circumvention activity or receiving circumvention assistance. The DMCA could also require the applicant to explicitly declare the reason for the application, the scope of the use he intends to make of the circumvention, and other required information in its application form. These forms and declarations could also be important evidence in litigation. Once the applicant's conduct goes beyond the declaration in her application, it may be easier to charge her with a violation of § 1201.

*D. General Advice for Future Legislators & the Multi-Level Role of Copyright Law in Future Legal Reform*

In general, this Article proposes that when future legislators deal with the problems brought by the current anti-circumvention provisions of the DMCA, it would be better to “think more holistically” and “not solely through the lens of the copyright law.”<sup>206</sup>

---

<sup>206</sup> See Samuelson, *More Sensible Regulations*, *supra* note 51, at 8 (“[I]t would be better to *think more holistically* about circumvention and circumvention technologies and



Recent cases in the U.S. have demonstrated that the problems brought by anti-circumvention provisions are not limited to copyright law issues.<sup>207</sup> Section 1201 also creates conflicts with other legislation, competition law, and consumer protection law.<sup>208</sup> Future anti-circumvention legislation must minimize these conflicts. This Article suggests that copyright law cannot, and should not, have to solve all of the problems by itself, and it would be better to seek for a multi-law solution. For example, antitrust law may be better equipped than copyright law to address these issues.

Nevertheless, copyright law should still play a very important role in the process of solving these problems. Copyright law can serve as a good jumping-off point for developing better anti-circumvention rules where a balance of benefits can be reached between all parties. First, the comprehensive balance theory of copyright law will provide a good theoretical foundation for future legislation reform. Second, copyright law can serve as a good platform for establishing new legal enforcement mechanisms. There are many well-established legal mechanisms existing in copyright law that may serve as good models for new legal enforcement mechanisms created to respond to the new problems brought by anti-circumvention rules. For example, the “notice and takedown regime” in the DMCA inspired the fair-circumvention application procedure proposed in this Article.<sup>209</sup> Third, copyright law can serve as a good platform for legislators to follow changes brought by technological developments. Copyright law not only

---

adopt a more general rule about them, so that the legitimacy of circumvention and circumvention technologies might be viewed more broadly, and *not solely through the lens of a copyright industry-oriented law.*”) (emphasis added). The author believes that this same logic can also be used broadly on anti-circumvention law issues, i.e. that it would be better to “think more holistically,” and not solely “through the lens of the copyright law” to seek solutions for the problems brought by anti-circumvention provisions of the DMCA.

<sup>207</sup> See *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000); see also *RealNetworks, Inc. v. Streambox, Inc.*, No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

<sup>208</sup> Section 1201 has been widely applied by the different entities (including non-copyright entities) in many non-copyright issues, such as anti-competition, privacy protection, and consumer protection issues. See *supra* Part III.E.4.

<sup>209</sup> See *supra* Part III.C.

has a long history,<sup>210</sup> but also always tries to closely follow the latest developments in technology, and adapt existing legislation to the challenges brought by new technologies. Finally, when exploring problems in a new and unfamiliar area, like cyber law or anti-circumvention law, it is good practice to start from a familiar area, and copyright law seems the best option.

### CONCLUSION

This Article has introduced and compared the anti-circumvention provisions in both the WIPO Internet Treaties and the Digital Millennium Copyright Act (DMCA). It also identified the major problems of the DMCA anti-circumvention provisions and examined the main reasons for those problems as illustrated by some recent cases. This Article then provided some specific suggestions for reforming the US anti-circumvention legislation.

As mentioned above, future legislators should think “more holistically and not solely through the lens of the copyright law”<sup>211</sup> when reforming anti-circumvention provisions of the DMCA. They should not only make use of current copyright law, but also try to take a more heterogeneous approach to solve its problems. Legislators should create new general legal principles, such as the proposed fair circumvention doctrine, and new legal enforcement procedures, such as the fair circumvention application procedures. They should also consider the discretionary power of the courts, market forces, and other possible methods that could all work together to deal with the challenges brought by anti-circumvention law, particularly the conflicts between anti-circumvention law and the rights permitted in existing legislation.

---

<sup>210</sup> The Statute of Anne was enacted in UK in 1710. See UK Intellectual Property, *A History of Copyright*, <http://www.intellectual-property.gov.uk/std/resources/copyright-history.htm> (last visited Jan. 6, 2005).

<sup>211</sup> See *supra* note 206.